Mitigating ROQ Attacks using Flow Monitoring Method

Seema Gulati [1], Amandeep Singh Dhaliwal[2]

[#1]*Research Scholar, CSE, RIMT-IET (PTU), Mandi Gobindgarh, India*

[#2]*Assistant Professor, CSE, RIMT-IET (PTU), Mandi Gobindgarh, India*

***Abstract*— Reduction of Quality attacks is a milder form of the DOS attacks but these are more difficult to detect than the traditional flooding attacks. The goal of these attacks do-not wish to completely cut-off services and resources or damage resources, instead only wish to reduce the QoS offered to the users of the systems and the services of the system. These attacks send traffic at a sufficiently low average rate to evade the detection systems, and try to keep the systems oscillate between over load and under load conditions. Unlike the traditional DOS attacks which limit the steady state capacity of a system, these target the adaptive behavior of the TCP congestion control mechanism. In this paper a flow monitoring technique is proposed to mitigate the impact of ROQ attacks in wireless networks. The simulation results show that the proposed technique helps to reduce packet loss and improves throughput.**

***Keywords*— ROQ, DDOS, Shrew, RTO, RTT, TCP time-out.**

I. INTRODUCTION

Denial of service attacks and its variants are a great threat to any kind of Internet service. MyDoom Company crashed SCO Group's website, by attacking it with a DDOS attack (Distributed Denial of Service). The attack involved 100-200k zombies (a huge number). It had cost the global economy about 26.1B ($). Reduction of Quality Attacks (ROQ pronounced as rock) are a new variant of the DDOS attacks which while keeping a low profile can easily cause a lethal blow to any system or service by targeting adaptation mechanisms. Most of the internet traffic (legitimate) and also the attack traffic apply the TCP protocol. It is very difficult in-fact not feasible to distinguish or segregate the malicious attack traffic from the legitimate TCP flows using only the protocol information embedded in the packet header. The traditional DDOS attacks are launched by sending high volume of traffic or requests to overwhelm the target and thus causing the system to crash down and deny the legitimate users of the intended services. A variant of the DOS Attacks had been discovered while causing a lethal blow to the end systems they try not to attract attention of the detection systems, thus surpassing most of the detection mechanisms. These attacks are named as ROQ (Reduction Of Quality) attacks, these aim to degrade the quality of a system or the services offered by it substantially, while trying to evade the detection system by posing as lawful users of the system.

II. DOS ATTACKS

There are many DOS attacks which target the capability of the end systems, and bleed the system capabilities. This is generally done by consuming or exhausting the resources of a system, the resources may be the bandwidth available, or the CPU resources such as CPU time and cycle. The other way to mount a DOS attack is tampering with important information such as the routing information or state information. The DOS attacks may also damage the physical components of a system.

A. Different DDOS Attack types

Flooding Attack which forces the victim to gradually end the communication with the neighboring nodes.

Self Whisper Attack selects two nodes randomly which keep sending traffic to each other for a random period.

Pulsing Attack selects a single node as an attacker and then sends it to randomly selected node (single target), and sends traffic to it for a random period and a random rate.

TCP reset sends fake TCP RESET requests after listening to the other TCP connections, thus causing end of the connections.

SYN flood sends fake TCP/SYN to the server, which is accepted by the server and then the server keeps waiting for the ACK packets which are never received.

ICMP Flooding Attack is launched by sending flood of echo-reply packets to random destinations, causing congestion in the network. Smurf, Ping Flood, Ping of Death are some of the ICMP Attacks.

Teardrop attack sends packets with tangled fragments of IP which have overlapping and oversized payloads, due to which the machines assume that they have an error in the TCP/IP fragmentation re-assembly code and the system crashes.

Permanent Denial of Service (PDOS) Attack target the vulnerabilities in the security mechanism and thus taking over the remote administration of the system, then the attacker causes damage to the physical resources such as routers, printers, etc. This is fatal at times and replacement of the hardware might be needed.

III. ROQ ATTACKS

ROQ attacks are a different kind of attacks which either result into over-utilization or under-utilization of the resources, they make the system oscillate between over-load or under-load conditions. The users of the system do-not get appropriate response time and services and thus get degraded quality of service (QoS).

ROQ attacks do-not overwhelm the sender by sending bulk instead the capture the loop holes of the adaptation mechanism (like the TCP-Time Out mechanism for congestion control).

The attack is mounted by sending burst of traffic to a target, which causes TCP to time-out. The TCP then triggers its Congestion Control algorithm, thus halving its sending rate. The sending of attack traffic is only for a very short interval of time, so now legitimate flow does not utilize the bandwidth available, assuming the link or the network to be congested. After waiting for some time, when the network starts converging, again the attack traffic is sent to the target to cause a Time-Out for a very short time period.

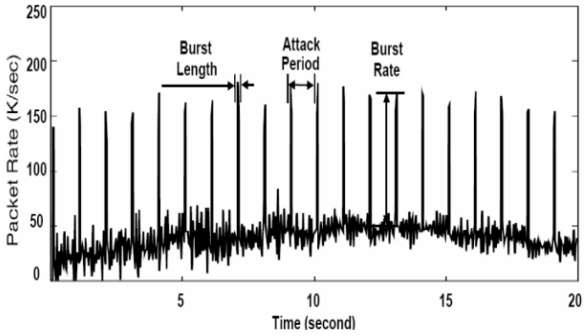

Fig 1 Example of TCP Traffic Flow mingled with Low Rate ROQ Attack traffic.

Attack definition The ROQ attacks are defined by the equation:

$$M = \delta\tau$$

where,
M represents the amount of burst sent (magnitude of the attack),
δ represents the rate of packets sent (amplitude of the attack),
τ represents the repetition period or the small attack period (duration of the attack).
The attack is repeated after every T units of time.

Attack Goal: the main aim of the attacker is to maximize the extent of damage caused to the system, with the help of the attack, while keeping the cost incurred to launch the attack to a limit. Hence the Attack Potency is defined as the ratio between the extents of damage caused to the system and the cost of launching that attack on the system.

$$\prod = \frac{Damage}{Cost^{\frac{1}{\Omega}}}$$

Here Ω represents the aggressiveness of the attacker. The damage and cost can vary according to the conditions (what an attacker wants to degrade). Various metrics which are used for measuring the extent of damage caused and the cost of mounting the attack are: Bandwidth, Delay, Jitter, etc.

A. Attack Orchestration

The ROQ Attacks do-not result into a complete refusal of the services, instead they strangulate the TCP throughput to a great extent and reducing the QoS (Quality of Service) offered gradually. These attacks are also termed as TCP Targeted Low Rate DDOS attacks by some researchers.

The TCP congestion control mechanism operates on two time scales: RTT and RTO. RTT is the time taken for the complete round trip i.e. from the sending of the packet to the receiving of the acknowledgement of the packet. RTO is a time period for which the sender shall wait for the acknowledgement of the packets it has sent. RTO is greater than the RTT. Whenever the packets are sent during a TCP connection, the sender shall wait for a time period of RTO to receive the acknowledgement of the packets being delivered at the destination. If the acknowledgement is not received within the RTO, the sender shall resend (*retransmission of packets*) the packets. In such a case the TCP sender Time-outs and assumes that there is congestion in the network and doubles its RTO and halves its sending rate. If packets are again not delivered then the RTO is again doubled, and the sending rate of the current sending rate. This is called AIMD (Additive Increase Multiplicative Increase) congestion control mechanism.

Example, A sends 20 packets to B then the RTO is equal to one second (RTO = 1s generally), the sender waits for one second to receive the acknowledgement of packets. Assume that the *ack packets* are not received within 1s. Then the sender enters a time-out state, and now the sender shall double its RTO to 2s, and reduces its sending rate to 10 packets. Now when the 10 packets are sent A shall wait for 2s (RTO = 2s). If again the packets are not acknowledged then the RTO is again doubled to 4s, and the retransmission of packets take place with halved rate that is 5 packets. But if the packets are

received this time then the RTO shall be halved to 2s, and sending rate shall be increased additively to 7 packets (assumption).

The ROQ attacks target this adaptation of TCP protocol. The sender chooses a busy and an optimal node (or a link) as a target which causes maximum damage to the network. The attack is mounted by sending burst of traffic on the target for a very short interval of time, causing the buffers/queues to overflow and thus causing time-out of the legitimate TCP flows. The legitimate connections after experiencing a time-out enter into the AIMD congestion control algorithm. Again when the legitimate connections resend the packets after RTO the attacker, sends the bursty attack traffic, causing again a time-out of the legitimate flows. Thus the throughput of the TCP is strangulated.

B. *Difference between Shrew and ROQ Attacks*

Some researchers place both the ROQ and shrew attacks under the same category but there is a minute difference between the two. The basic difference lies between the repetition of the attack that is the interval between each δ units of attack traffic sent by the attacker. In Shrew Attacks the Attack period (T) is close to the RTO (generally equal to the RTO). But, in the ROQ Attacks the attack period (T) is longer and random. Due to the varying time period, the network might converge in between the two bursts, but in shrew attacks the network is not allowed to converge. Thus the shrew attack may prove to be fatal at times.

IV. Related Work:

Y. Xu et al [4] proposed a queue management technique i.e. RED algorithm and the RED-PD algorithm. The RED (Random early detection) congestion control mechanism monitors the average queue size for each output queue using randomization.

Amey Shevtekar et al [5] designed a detection algorithm for low rate TCP denial of service attack detection at edge routers. A new data structure (light-weight) was introduced to store the necessary history of the edge routers.

Amey Shevtekar et al [6] also proposed a router based technique to mitigate the reduction of quality (ROQ) attacks. The proposed system works in two phases: Detection and Filtering. Detection was based on per flow information.

Yu Chen at al [7] proposed a new signal-processing approach to identify and detect the attacks by examining the frequency domain characteristics of incoming traffic flows to a server. The technique is produces a solution in a very short period of a few seconds.

Yu Chen et al [8] have proposed a defense approach on the basis of the energy distributions; the TCP flows present a periodicity in the traffic pattern due to the TCP protocol behavior. Normal TCP flows can be separated from attack traffic using the energy distribution properties. The defense strategy combines both flow level spectral analysis and the sequential hypothesis testing.

Jatinder Singh et al [9] proposed a defense scheme that detects the attack traffic on the basis of values obtained from the MAC layer. The detection stage uses three values: 1.Frequency of RTS/CTS packets, 2. Frequency of sensing a busy channel and 3. Number of RTS/DATA transmissions. The three values are used to set a congestion bit which is used to draw conclusions, whether or not the traffic is from an attacker.

V. Proposed Defense Technique:

In this technique an Attack Monitor is selected, which is used as a controller for the detection mechanism.

The Attack Monitor is selected on the basis of a factor, X:

$$X = \{(Ql + Qc) / D\} E$$

Where, Ql is the quality of link, Qc is the quality of channel, D is the average delay incurred and E is the Residual Energy. The node, for which the value of factor X comes is maximum, it is selected as the Attack Monitor for Detection.

Algorithm:

Let L be the Last Accessed Time, Cr be the Creation Time of the flows coming on the nodes on the network. Let A be the set of all short lived flows and Cu be the current time.

1. Select an ATTACK MONITOR

2. If a sudden increase in traffic flow is detected which causes congestion for a very short time.

a. For all flows € {A}

If (L-Cr) = Cu-1,

then $\text{Total} = \sum_{F=1}^{N} \text{load}$

b. If total > limiting threshold value then the node is a POTENTIAL ATTACKER

c. Add all such nodes into a list of suspicious nodes.

3. Send Suspicious List to Attack Monitor

4. Attack Monitor compares the lists

a. If a name appears more than a number of times, Then Add the node to the CHECKING TABLE

b. Communicate the Checking Table to all nodes.

6. At the nodes:

a. Drop all packets currently
b. Start monitoring these nodes
c. If incoming flow > Threshold
then counter 1++

Else counter 2++

d. After a chosen time period compare the counters
If counter 1 >> counter 2

then declare the node as attacker and add into the ATTACKER TABLE.

Else remove from Checking Table

7. Block all the traffic from the nodes in the ATTACKER TABLE.

VI. SIMULATION RESULTS:

In this section experimental performance evaluation of the proposed algorithm is shown with the help of simulations. To simulate the given algorithm on a wireless network OPNET Modeler was used. The OPNET is a very powerful network simulator. Main purposes are to optimize cost, performance and availability. It has a very fast discrete event simulation engine and is used among leading industry solutions and Integrated, GUI-based debugging and analysis. The graphs shown here are for 2 (A2 DES-1), 4(A4 DES-1), 6 (A6 DES-1) attackers.

No of Nodes	30
Area	100 m * 100 m
Bandwidth	512 kb
MAC	802.16
Simulation Time	300 sec
Values per Statistic	100
Update Interval	50000 events
Creation Source	ETS
Attackers	2,4,6

Table I
Simulation Parameters

Above table shows the simulation parameters (assumptions) and the figures below show the results. The graphs shown here are for 2 (A2 DES-1), 4(A4 DES-1), 6 (A6 DES-1) attackers.

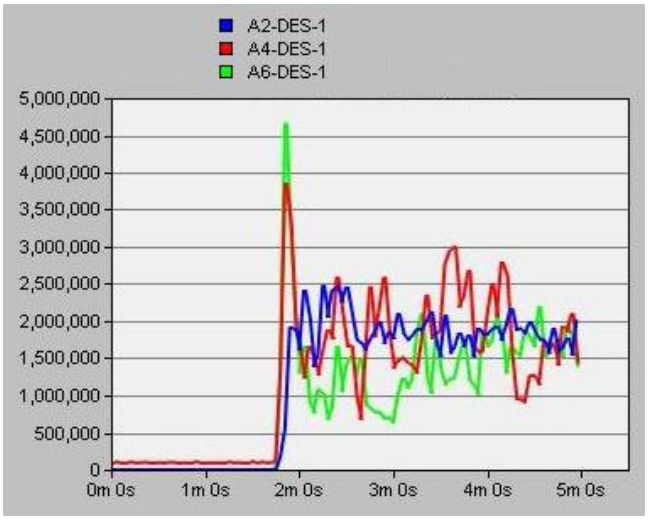

Fig 2 Throughput (bits per second)

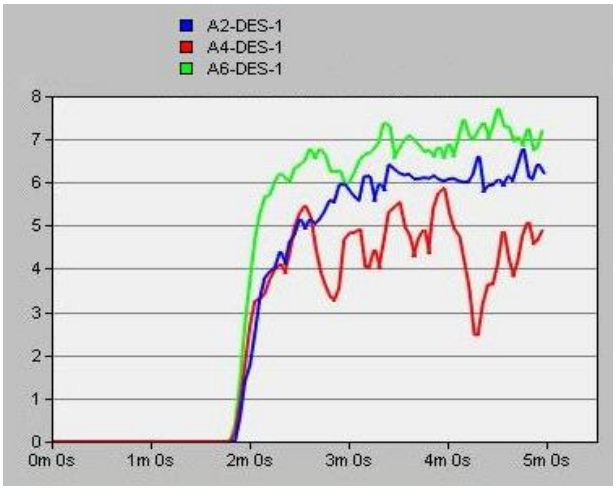

Fig 3 Retransmission Attempts

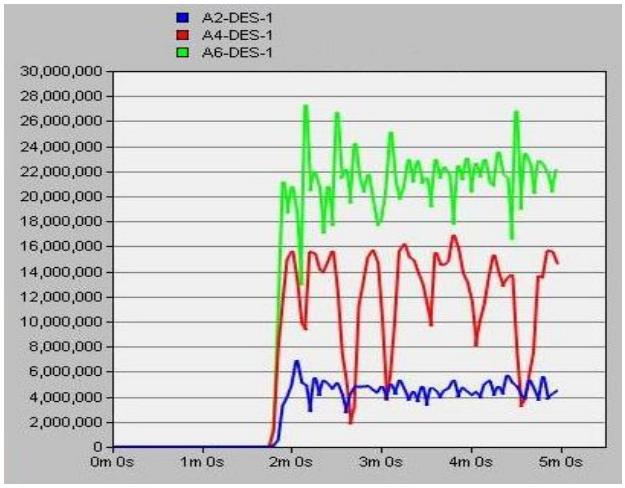

Fig 4 Delay (sec)

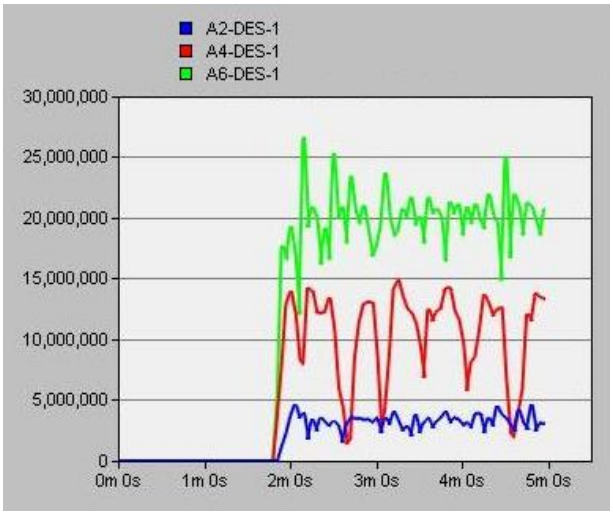

Fig 5 Load (bits/sec)

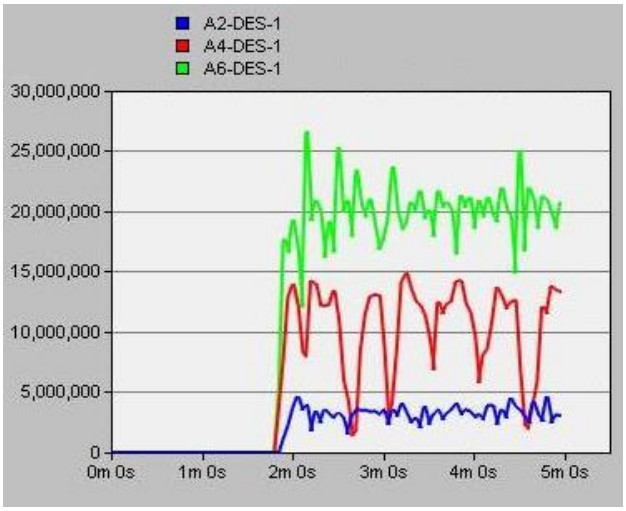

Fig 6 Data Dropped (Buffer Overflow) (bits/sec)

CONCLUSION

The paper looks into the current techniques to mitigate ROQ Attacks, and focuses on a flow monitoring technique. In this technique all the nodes in the system is checked after every unit time for flows which last for a very short unit of time and exceed a certain threshold value. Such nodes are into a data structure and then all nodes compare this data structure for possible attacking nodes. If a node appears in more than a certain number of times it is said to be a potential attacker, all further traffic is blocked from such nodes. Then the flow from these nodes is again monitored, if they keep sending bursts then they are declared as attackers and permanently blocked. The simulation results show that the proposed technique helps to reduce packet loss and improves throughput.

REFERENCES

[1] A. Kuzmanovic and E. Knightly, "Low-rate TCP-targeted denial of service attacks (The Shrew vs. the Mice and Elephants)", ACM SIGCOMM 2003, pp. 75–86, 2003.

[2] Mina Guirguis, Azer Bestavros and Ibrahim Matta, "Exploiting the transients of adaptation for RoQ attacks on Internet resources", IEEE ICNP 2004, pp. 184–195, 2004.

[3] Mina Guirguis, Azer Bestavros and Ibrahim Matta, "Bandwidth Stealing via Link Targeted RoQ Attacks", IEEE CCN 2004, 2004.

[4] Y. Xu, R. Guerin, "On the robustness of router-based denial-of-service (DoS) defense systems", ACM Computer Communications, Vol. 35, No. 3, pp. 47–60, 2005.

[5] Amey Shevtekar, Karunakar Anantharam, and Nirwan Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers", IEEE Communications Letters, Vol. 9, No. 4, April 2005.

[6] Amey Shevtekar and Nirwan Ansari, A router based technique to mitigate reduction of quality (RoQ) attacks, Computer Networks, Vol. 52, pp. 957–970, 2008.

[7] Yu Chen, Kai Hwang," Collaborative detection and filtering of Shrew DDoS attacks using spectral analysis", Journal of Parallel and Distributed Computing, Special Issue on Security in Grids and Distributed Systems, Vol. 66, No. 9, 2006.

[8] Yu Chen and Kai Hwang, "Spectral Analysis of TCP flows for Defense against Reduction-of-Quality Attacks", IEEE International Conference on Communications (ICC 2007), 2007.

[9] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN", International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[10] Rupa Rani and A.K. Vatsa, "CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET", International Journal of Engineering and Technology, Volume 2 No. 8, August, 2012.

[11] S. Venkatasubramanian and N. P. Gopalan, "A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET", International Journal of Computer Applications (0975 – 8887), Volume 21– No.1, May 2011.

[12] S. A. Arunmozhi and Y. Venkataramani, "A Flow Monitoring Scheme to Defend Reduction-of-Quality (RoQ) Attacks in Mobile Ad-hoc Networks", Information Security Journal: A Global Perspective, Vol.19, No.5, 2010, pp. 263- 272.

[13] Arunmozhi Annamalai and Venkataramani Yegnanarayanan, "Secured System against DDoS Attack in Mobile Adhoc Network", WSEAS Transactions on Communications, Issue 9, Volume 11, September 2012

[14] K. Kuppusamy and S. Malathi, "An Effective Prevention Of Attacks Using GI Time Frequency Algorithm Under DDOS", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.